RSAC 2025 Conference

Many Voices.
One Community.

SESSION ID: LAW-T09

Boards and C-Suites: Are These the Droids You're Looking For?

MODERATOR:

Erez Liebermann
Partner
Debevoise & Plimpton LLP

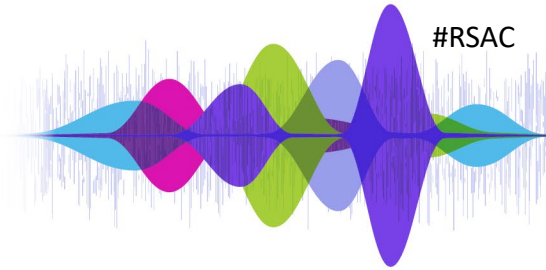
PANELISTS:

Alison Atkins
Chief Cyber Security and Technology Counsel
U.S. Bank

Tom Doughty
Chief Information Security Officer
Generate Biomedicines

Matt Greenberg
Assistant General Counsel, Executive Director – Cybersecurity & Incidence Response
Wells Fargo

Disclaimer



Presentations are intended for educational purposes only and do not replace independent professional judgment. Statements of fact and opinions expressed are those of the presenters individually and, unless expressly stated to the contrary, are not the opinion or position of RSA Conference LLC or any other co-sponsors. RSA Conference LLC does not endorse or approve, and assumes no responsibility for, the content, accuracy or completeness of the information presented.

Attendees should note that sessions may be audio- or video-recorded and may be published in various media, including print, audio and video formats without further notice. The presentation template and any media capture are subject to copyright protection.

© 2025 RSA Conference LLC or its affiliates. The RSAC and RSAC CONFERENCE logos and other trademarks are proprietary. All rights reserved.

RSAC 2025 Conference

#RSAC

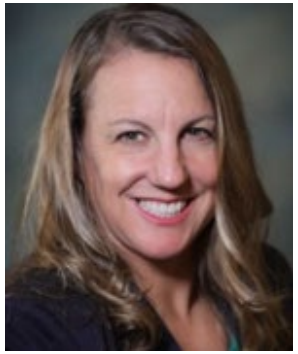
Many Voices.
One Community.

MODERATOR:

Erez Liebermann

Partner
Debevoise & Plimpton LLP

PANELISTS:



Alison Atkins

Chief Cyber Security and Technology Counsel
U.S. Bank

Tom Doughty

Chief Information Security Officer
Generate Biomedicines

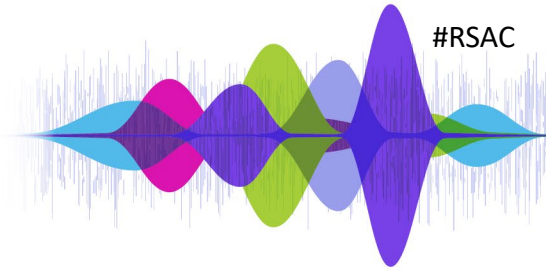
Matt Greenberg

Assistant General Counsel, Executive Director – Cybersecurity & Incidence Response
Wells Fargo

Key Takeaways

- Cybersecurity is a Board-Level Responsibility, Not Just a Management Responsibility
- Proactive Preparedness Can Reduce Legal and Financial Exposure
- Post-Incident Reviews are Critical for Future Resilience

Board's Role Regarding Cyber Governance



- OVERSIGHT

✓Ensure appropriate time, staff, and financial resources are devoted to cybersecurity program

✓Provide valuable cybersecurity expertise and cross-industry perspectives

- RISK MANAGMENT

✓Assess and manage cybersecurity risk tolerance

✓Ensure business decisions reflect agree-upon risk tolerances

✓Support management during incident response to mitigate post-incident business, regulatory, and litigation risks

- COMPLIANCE

✓Ensure board governance complies with applicable regulations

✓Oversee cybersecurity policies and procedures to ensure compliance with ever-evolving regulatory requirements

Basics and Best Practices

Identify Ownership. Clearly identify who is responsible for managing cybersecurity risk throughout the organization.

Task a Board Committee. Explicitly assign cybersecurity risk responsibility to a relevant committee (typically Audit or Risk).

Schedule Regular Briefings. Put security on board and committee agenda. Full board annually, committee quarterly, at minimum.

Conduct Briefs. Assign briefings to a qualified individual responsible for overseeing, implementing, and enforcing cybersecurity (CISO or equivalent).

Understand Risk. Assess and understand the financial, operational, and reputational risks associated with a cybersecurity incident.

Determine Tolerances. Evaluate if organization is taking on right level of risk, or too much. Monitor risk reduction.

Review Policies and Procedures. Ensure familiarity with key cybersecurity policies, including the Incident Response Plan.

Prepare for an Incident. Understand a director's role before, during, and after a cyber breach. Confirm the organization has cyber insurance.

Red Flags to Watch for During Briefings

Self-Licking Ice Cream Cone

Internal self-assessments without external validation

All Green

“Everything is going great!”

The Pen(test) is Mightier

Not enough to have flawless written policies and procedures if you never put them to the test

Castle Mentality

High walls, wide moat, but weak internal defense system

CISO to the Rescue

The prior CISO did everything wrong and only the current CISO can fix it

All Hat, No Cowboy

Subjective analysis and story telling not backed up by objective data and evidence

Green Flags to Observe During Briefings

Consistent Messaging

Uses a common framework to manage and communicate program

Uses Independent testing

Leverages third parties and communicates results

Plain English

Translates cyber risk into understandable terms and inspires confidence while still being able to message bad news

Measured Approach

Effectively prioritizes and executes against priorities; balances business needs with risk

Metrics Driven

Uses data to measure risk and return on investment

Assumes a Breach

Assumes breaches are “when not if” events and adopts policies and procedures aimed at containing them

PRIVILEGED & CONFIDENTIAL

The Board's Role During an Incident

Connection Points with The Board	Evolving Practices
When does the board get engaged?	• Boards are proactively engaged in managing cyber risk • Executive Team engages the board during cyber events
How does the board get engaged?	• Designated Cyber Board Liaison(s) are proactively engaged to gain a deeper understanding of cyber risk • A single designated senior leader (i.e., Chief Executive Officer) informs the board of a significant cyber event and provides ongoing updates • Cyber Board Liaison(s) have ongoing deeper discussions on cyber events for support to the broader board
What does the board do?	• Provide oversight and insight to the Executive Team

Board of Directors

- Provide a shareholder's perspective into critical decisions
- Bring a broader, cross-industry lens to the cyber event (including companies that may have undergone a crisis)
- Provide general guidance and council on legal, financial, regulatory, and communications, as appropriate
- Understand that the situation will be rapidly evolving and the Executive Team may not have all the information available
- Understand the limitations and protocols around communications and the importance of controlling the message—the actions taken and decisions made in the early hours of a cyber event can significantly impact stakeholder confidence
- Be vigilant about how you protect, share, and manage sensitive incident data / information to maintain privilege and confidentiality

Executive Team

After an Incident

Investigation	Debrief	Lessons Learned	Personnel Changes	Peacetime Prep
Consider whether a board investigation is warranted (different than incident response)	Ensure board receives thorough debrief during Recover Phase	Understand key lessons learned and timetable for updates to cyber program	If necessary, support and help make difficult personnel changes	Where are we at now and how are we measuring ourselves? Risks and areas for improvement?

RSAC™ 2025 Conference

Many Voices.
One Community.

Thank You